The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/28/2009

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox and SeaMonkey Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Mozilla Firefox and Mozilla SeaMonkey applications which could allow remote code execution. Mozilla Firefox is a popular web browser used to access the Internet. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client.

The Mozilla applications (Firefox and SeaMonkey) utilize the same framework to display application specific information (e.g. Web pages, emails, chats). Exploitation can occur if a user visits a webpage or opens a malicious file specifically crafted to take advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Mozilla Firefox versions 3.5.3 and earlier
Mozilla SeaMonkey versions 1.1.17 and earlier

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla Seamonkey that could allow an attacker to take complete control of an affected system. Details of these vulnerabilities are:

Form History vulnerable to stealing

An information disclosure vulnerability exists which could allow for the disclosure of history content. The problem occurs because a malicious web page could synthesize mouse movement and key press events to auto-populate form fields with history entries. Information obtained may aid in further attacks.

Crash with Recursive Web-Worker Calls

An arbitrary code execution vulnerability exists due to a recursive creation of JavaScript web-workers. An attacker can exploit this issue to free object memory before it is used. This will likely cause denial-of-service conditions; arbitrary code execution may also be possible.

Crash in Proxy Auto-configuration Regexp Parsing

An arbitrary code execution vulnerability exists due to a flaw in parsing regular expressions used in Proxy Auto-configuration (PAC) files. An attacker can exploit this issue to crash a victim's browser, and possibly run arbitrary code.

Heap Buffer Overflow in GIF Color Map Parser

A heap-buffer overflow vulnerability exists in the GIF color map image parser. An attacker can exploit this issue to execute arbitrary code in the context of the victim running the affected browser.

Chrome Privilege Escalation in XPCVariant::VariantDataToJS()

A privilege-escalation vulnerability affects the XPCOM utility 'XPCVariant::VariantDataToJS()' because it doubly-wraps objects before returning them to chrome callers. An attacker can exploit this issue to execute malicious JavaScript with chrome privileges.

Local Downloaded File Tampering

A local privilege-escalation vulnerability occurs because the browser uses predictable names when downloading and saving files to the ‘Downloads’ folder. An attacker with local access, and knowledge of a file a victim intends to open with Download Manager, could exploit this issue to execute a malicious file in the context of the victim running the affected browser.

Heap Buffer Overflow in String to Number Conversion

A heap-based buffer overflow vulnerability in the string to floating point number conversion routines. An attacker can exploit this issue by tricking an unsuspecting victim into viewing a malicious web page containing specially crafted JavaScript. A successful exploit will result in the execution of arbitrary code on the victim's computer.

Cross-origin Data Theft through document.getSelection()

A cross-domain information disclosure vulnerability occurs because text within a selection on a web page can be read by JavaScript in a different domain using the 'document.getSelection' function.

Download Filename Spoofing with RTL Override
A vulnerability occurs that could allow an attacker to obfuscate the name and file extension of a file to be downloaded. The problem occurs when the file contains a right-to-left override character (RTL) in the filename.

Memory Safety Bugs
A remote code execution vulnerability affects the third-party 'liboggz', ‘libvorbis’, and ‘liboggplay’ libraries used in Firefox. This issue can be exploited to cause the browser to crash; arbitrary code execution may also be possible.

Crashes with Evidence of Memory Corruption
Multiple remote memory corruption vulnerabilities affect Firefox. These issues can be exploited to
cause the browser to crash and possibly to execute arbitrary code.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Install the appropriate vendor patches and upgrades immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Secunia:
http://secunia.com/advisories/36711/

Security Focus:
http://www.securityfocus.com/bid/36843

Mozilla:
http://www.mozilla.org/security/announce/2009/mfsa2009-52.html
http://www.mozilla.org/security/announce/2009/mfsa2009-53.html
http://www.mozilla.org/security/announce/2009/mfsa2009-54.html
http://www.mozilla.org/security/announce/2009/mfsa2009-55.html
http://www.mozilla.org/security/announce/2009/mfsa2009-56.html
http://www.mozilla.org/security/announce/2009/mfsa2009-57.html
http://www.mozilla.org/security/announce/2009/mfsa2009-59.html

http://www.mozilla.org/security/announce/2009/mfsa2009-61.html
http://www.mozilla.org/security/announce/2009/mfsa2009-62.html
http://www.mozilla.org/security/announce/2009/mfsa2009-63.html
http://www.mozilla.org/security/announce/2009/mfsa2009-64.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1563
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3370
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3372
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3374
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3376
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3378
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3380
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3382
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3274
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3371
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3373
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3375
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3377
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3379
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3381
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3383